November 18th, 2021

EXERCISES SESSION — MPRI C-2-22

In what follows, $\mathbb{K}$ denotes an effective field of characteristic zero.

1. Computation of symmetric polynomials

Let $x_1, x_2, \ldots, x_n$ be elements of $\mathbb{K}$ and, for $k \geq 1$, let

$$e_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} \qquad \text{and} \qquad p_k = \sum_{i=1}^{n} x_i^k$$

be the power sums and the elementary symmetric polynomials in these elements.

(a) Give a first algorithm for the computation of $\mathbf{p} := (p_1, \ldots, p_n) \in \mathbb{K}^n$, relying on the definition of p_k, and estimate its arithmetic complexity.
(b) Same question for the computation of $\mathbf{e} := (e_1, \ldots, e_n) \in \mathbb{K}^n$.
(c) Design an algorithm that computes $\mathbf{e}$ in $O(\mathsf{M}(n) \log n)$ operations in $\mathbb{K}$.
(d) Same question for the computation of $\mathbf{p}$. [Hint: introduce a suitable generating function.]

2. Composition with the exponential

Let $f(X) \in \mathbb{K}[[X]]$ and let $e(X) \in \mathbb{K}[[X]]$ be the power series $e(X) = \exp(X) - 1 = \sum_{k \geq 1} X^k/k!$. The aim of this exercise is to propose an efficient algorithm for computing the first $N \in \mathbb{N}$ coefficients of the composition $h(X) := f(e(X))$, starting from the first N terms of $f(X)$.

(a) Design a direct algorithm for computing the first N coefficients of $h(X)$, and analyze its arithmetic complexity.

Let $A(X)$ be the polynomial of degree less than N such that $f(X) = A(X) + O(X^N)$.

(b) Let $B(X) = A(X-1)$ and define $\mathcal{L} : \mathbb{K}[[X]] \to \mathbb{K}[[X]]$ to be the $\mathbb{K}$-linear map such that $\mathcal{L}(X^k) = k!\, X^k$ for all $k \in \mathbb{N}$. Prove that $\mathcal{L}(B(\exp(X)))$ is a rational power series, and express it in terms of the coefficients of B.
(c) Design an algorithm for computing the first N coefficients of $B(\exp(X))$, starting from those of $B(X)$, in $O\big(\mathsf{M}(N) \log N\big)$ operations in $\mathbb{K}$.
(d) Propose finally an algorithm for computing the first N coefficients of $h(X)$, starting from those of $f(X)$, in $O\big(\mathsf{M}(N) \log N\big)$ operations in $\mathbb{K}$.

3. Graeffe polynomials

Let $f \in \mathbb{K}[X]$ be monic of degree $d \geq 1$. For $N \geq 1$, we denote by $G_N(f)$ the unique monic polynomial of degree d in $\mathbb{K}[X]$, whose roots are the N-th powers of the roots (in $\overline{\mathbb{K}}$) of f.

(a) Express $G_N(f)$ using a resultant of bivariate polynomials.
(b) Justify why all the coefficients of $G_N(f)$ belong to $\mathbb{K}$.
(c) Use (a) to design an algorithm that computes $G_N(f)$; estimate its arithmetic complexity in terms of N and d.
(d) Show that $G_2(f)$ can be computed in $O(\mathsf{M}(d))$ operations in $\mathbb{K}$.
(e) If N is a power of 2, show that one can compute $G_N(f)$ in $O(\mathsf{M}(d) \log(N))$ operations in $\mathbb{K}$.

4. Inversion of polynomial matrices by Strassen's algorithm

Let $M(X) \in \mathcal{M}_n(\mathbb{K}[[X]]_{\leq d})$ be an invertible polynomial matrix. Assume that one computes the inverse M^{-1} by using Strassen's inversion algorithm for dense (scalar) matrices.

Estimate the complexity of this computation, counting operations in $\mathbb{K}$, in terms of the two parameters n and d, under the assumption that all matrices encountered during the inversion algorithm are invertible.

5. On factoring polynomials over finite fields

Let p be an odd prime number, let $n \in \mathbb{N}$ and $q = p^n$. Let $f \in \mathbb{F}_q[X]$ be a non-constant squarefree polynomial. Set $V = \mathbb{F}_q[X]/(f)$ and let $Q : V \to V$ be the $\mathbb{F}_q$-linear map given by $\eta \mapsto \eta^q$.

(1) Show that the number of irreducible factors of f is equal to the dimension of $\ker(Q - \mathrm{id})$ over $\mathbb{F}_q$. [Hint: start with the case when f is irreducible.]

(2) Let $\eta = v + (f) \in \ker(Q - \mathrm{id})$. Prove that $f = \gcd(f, v)\gcd(f, v^{\frac{q-1}{2}} - 1)\gcd(f, v^{\frac{q-1}{2}} + 1)$.

(3) Assuming that f is not irreducible, show that the factorization above is non-trivial for at least half of the η's in $\ker(Q - \mathrm{id})$.

(4) Using the previous questions, propose an algorithm that takes $f \in \mathbb{F}_q[X]$ as input and that either proves that f is irreducible, or returns a non-trivial factor of it. Analyze the arithmetic and the bit complexity of the proposed algorithm.